About the security content of macOS Sonoma 14.7.5

This document describes the security content of macOS Sonoma 14.7.5.

About Apple security updates

For our customers' protection, Apple doesn't disclose, discuss, or confirm security issues until an investigation has occurred and patches or releases are available. Recent releases are listed on the Apple security releases page.

Apple security documents reference vulnerabilities by CVE-ID when possible.

For more information about security, see the Apple Product Security page.

macOS Sonoma 14.7.5

Released March 31, 2025

AccountPolicy

Available for: macOS Sonoma

Impact: A malicious app may be able to gain root privileges

Description: This issue was addressed by removing the vulnerable code.

CVE-2025-24234: an anonymous researcher

AirDrop

Available for: macOS Sonoma

Impact: An app may be able to read arbitrary file metadata

Description: A permissions issue was addressed with additional restrictions.

CVE-2025-24097: Ron Masas of BREAKPOINT.SH

AirPlay

Available for: macOS Sonoma

Impact: An attacker on the local network may be able to cause a denial-of-service

Description: A null pointer dereference was addressed with improved input validation.

CVE-2025-24177: Uri Katz (Oligo Security)

CVE-2025-24179: Uri Katz (Oligo Security)

Entry added April 28, 2025

AirPlay

Available for: macOS Sonoma

Impact: An attacker on the local network may cause an unexpected app termination

Description: The issue was addressed with improved checks.

CVE-2025-24251: Uri Katz (Oligo Security)

CVE-2025-31197: Uri Katz (Oligo Security)

Entry added April 28, 2025

AirPlay

Available for: macOS Sonoma

Impact: An attacker on the local network may be able to bypass authentication policy

Description: An authentication issue was addressed with improved state management.

CVE-2025-24206: Uri Katz (Oligo Security)

Entry added April 28, 2025

AirPlay

Available for: macOS Sonoma

Impact: An attacker on the local network may be able to corrupt process memory

Description: An input validation issue was addressed.

CVE-2025-24126: Uri Katz (Oligo Security)

Entry added April 28, 2025

AirPlay

Available for: macOS Sonoma

Impact: An unauthenticated user on the same network as a signed-in Mac could send it AirPlay commands without pairing

Description: An access issue was addressed with improved access restrictions.

CVE-2025-24271: Uri Katz (Oligo Security)

Entry added April 28, 2025

AirPlay

Available for: macOS Sonoma

Impact: An attacker on the local network may be able to leak sensitive user information

Description: This issue was addressed by removing the vulnerable code.

CVE-2025-24270: Uri Katz (Oligo Security)

Entry added April 28, 2025

AirPlay

Available for: macOS Sonoma

Impact: An attacker on the local network may be able to cause a denial-of-service

Description: The issue was addressed with improved memory handling.

CVE-2025-24131: Uri Katz (Oligo Security)

Entry added April 28, 2025

AirPlay

Available for: macOS Sonoma

Impact: An attacker on the local network may cause an unexpected app termination

Description: A type confusion issue was addressed with improved checks.

CVE-2025-24129: Uri Katz (Oligo Security)

CVE-2025-30445: Uri Katz (Oligo Security)

Entry added April 28, 2025

AirPlay

Available for: macOS Sonoma

Impact: An attacker on the local network may be able to corrupt process memory

Description: A use-after-free issue was addressed with improved memory management.

CVE-2025-24252: Uri Katz (Oligo Security)

Entry added April 28, 2025

App Store

Available for: macOS Sonoma

Impact: A malicious app may be able to access private information

Description: This issue was addressed by removing the vulnerable code.

CVE-2025-24276: an anonymous researcher

Apple Account

Available for: macOS Sonoma

Impact: An attacker in a privileged network position may be able to track a user's activity

Description: The issue was addressed with improved handling of protocols.

CVE-2024-40864: Wojciech Regula of SecuRing (wojciechregula.blog)

Entry updated April 2, 2025

AppleMobileFileIntegrity

Available for: macOS Sonoma

Impact: An app may be able to modify protected parts of the file system

Description: The issue was addressed with improved checks.

CVE-2025-24272: Mickey Jin (@patch1t)

CVE-2025-24231: Claudio Bozzato and Francesco Benvenuto of Cisco Talos

AppleMobileFileIntegrity

Available for: macOS Sonoma

Impact: A malicious app may be able to read or write to protected files

Description: A permissions issue was addressed with additional restrictions.

CVE-2025-24233: Claudio Bozzato and Francesco Benvenuto of Cisco Talos.

AppleMobileFileIntegrity

Available for: macOS Sonoma

Impact: An app may be able to access user-sensitive data

Description: A privacy issue was addressed by removing the vulnerable code.

CVE-2025-30443: Bohdan Stasiuk (@bohdan_stasiuk)

Audio

Available for: macOS Sonoma

Impact: Processing a maliciously crafted file may lead to arbitrary code execution

Description: The issue was addressed with improved memory handling.

CVE-2025-24243: Hossein Lotfi (@hosselot) of Trend Micro Zero Day Initiative

Audio

Available for: macOS Sonoma

Impact: Processing a maliciously crafted font may result in the disclosure of process memory

Description: The issue was addressed with improved memory handling.

CVE-2025-24244: Hossein Lotfi (@hosselot) of Trend Micro Zero Day Initiative

Automator

Available for: macOS Sonoma

Impact: An app may be able to access protected user data

Description: A permissions issue was addressed by removing vulnerable code and adding additional checks.

CVE-2025-30460: an anonymous researcher

BiometricKit

Available for: macOS Sonoma

Impact: An app may be able to cause unexpected system termination

Description: A buffer overflow was addressed with improved bounds checking.

CVE-2025-24237: Yutong Xiu

Calendar

Available for: macOS Sonoma

Impact: An app may be able to break out of its sandbox

Description: A path handling issue was addressed with improved validation.

CVE-2025-30429: Denis Tokarev (@illusionofcha0s)

Calendar

Available for: macOS Sonoma

Impact: An app may be able to break out of its sandbox

Description: This issue was addressed with improved checks.

CVE-2025-24212: Denis Tokarev (@illusionofcha0s)

CloudKit

Available for: macOS Sonoma

Impact: A malicious app may be able to access private information

Description: The issue was addressed with improved checks.

CVE-2025-24215: Kirin (@Pwnrin)

CoreAudio

Available for: macOS Sonoma

Impact: Playing a malicious audio file may lead to an unexpected app termination

Description: An out-of-bounds read issue was addressed with improved input validation.

CVE-2025-24230: Hossein Lotfi (@hosselot) of Trend Micro Zero Day Initiative

CoreMedia

Available for: macOS Sonoma

Impact: A malicious application may be able to elevate privileges. Apple is aware of a report that this issue may have been actively exploited against versions of iOS before iOS 17.2.

Description: A use after free issue was addressed with improved memory management.

CVE-2025-24085

CoreMedia

Available for: macOS Sonoma

Impact: An app may be able to access sensitive user data

Description: An access issue was addressed with additional sandbox restrictions.

CVE-2025-24236: Csaba Fitzl (@theevilbit) and Nolan Astrein of Kandji

CoreMedia

Available for: macOS Sonoma

Impact: Processing a maliciously crafted video file may lead to unexpected app termination or corrupt process memory

Description: The issue was addressed with improved memory handling.

CVE-2025-24190: Hossein Lotfi (@hosselot) of Trend Micro Zero Day Initiative

CoreMedia

Available for: macOS Sonoma

Impact: Processing a maliciously crafted video file may lead to unexpected app termination or corrupt process memory

Description: This issue was addressed with improved memory handling.

CVE-2025-24211: Hossein Lotfi (@hosselot) of Trend Micro Zero Day Initiative

CoreMedia Playback

Available for: macOS Sonoma

Impact: A malicious app may be able to access private information

Description: A path handling issue was addressed with improved validation.

CVE-2025-30454: pattern-f (@pattern_F_)

CoreServices

Available for: macOS Sonoma

Impact: An app may be able to access sensitive user data

Description: This issue was addressed through improved state management.

CVE-2025-31191: Jonathan Bar Or (@yo_yo_yo_jbo) of Microsoft, and an anonymous researcher

CoreServices

Available for: macOS Sonoma

Impact: An app may be able to gain root privileges

Description: A logic issue was addressed with improved file handling.

CVE-2025-24170: YingQi Shi (@Mas0nShi) of DBAppSecurity's WeBin lab and Minghao Lin (@Y1nKoc), Stephan Casas

CoreUtils

Available for: macOS Sonoma

Impact: An attacker on the local network may be able to cause a denial-of-service

Description: An integer overflow was addressed with improved input validation.

CVE-2025-31203: Uri Katz (Oligo Security)

Entry added April 28, 2025

Crash Reporter

Available for: macOS Sonoma

Impact: An app may be able to gain root privileges

Description: A parsing issue in the handling of directory paths was addressed with improved path validation.

CVE-2025-24277: Csaba Fitzl (@theevilbit) of Kandji and Gergely Kalman (@gergely_kalman), and an anonymous researcher

curl

Available for: macOS Sonoma

Impact: An input validation issue was addressed

Description: This is a vulnerability in open source code and Apple Software is among the affected projects. The CVE-ID was assigned by a third party. Learn more about the issue and CVE-ID at cve.org.

CVE-2024-9681

Disk Images

Available for: macOS Sonoma

Impact: An app may be able to break out of its sandbox

Description: A file access issue was addressed with improved input validation.

CVE-2025-24255: an anonymous researcher

DiskArbitration

Available for: macOS Sonoma

Impact: An app may be able to gain root privileges

Description: A permissions issue was addressed with additional restrictions.

CVE-2025-24267: an anonymous researcher

DiskArbitration

Available for: macOS Sonoma

Impact: An app may be able to gain root privileges

Description: A parsing issue in the handling of directory paths was addressed with improved path validation.

CVE-2025-30456: Gergely Kalman (@gergely_kalman)

Dock

Available for: macOS Sonoma

Impact: A malicious app may be able to access private information

Description: The issue was addressed with improved checks.

CVE-2025-30455: Mickey Jin (@patch1t), and an anonymous researcher

Dock

Available for: macOS Sonoma

Impact: An app may be able to modify protected parts of the file system

Description: This issue was addressed by removing the vulnerable code.

CVE-2025-31187: Rodolphe BRUNETTI (@eisw0lf) of Lupus Nova

dyld

Available for: macOS Sonoma

Impact: Apps that appear to use App Sandbox may be able to launch without restrictions

Description: A library injection issue was addressed with additional restrictions.

CVE-2025-30462: Pietro Francesco Tirenna, Davide Silvetti, Abdel Adim Oisfi of Shielder (shielder.com)

Foundation

Available for: macOS Sonoma

Impact: An app may be able to cause a denial-of-service

Description: An uncontrolled format string issue was addressed with improved input validation.

CVE-2025-24199: Manuel Fernandez (Stackhopper Security)

Foundation

Available for: macOS Sonoma

Impact: An app may be able to access sensitive user data

Description: The issue was resolved by sanitizing logging

CVE-2025-30447: LFY@secsys from Fudan University

GPU Drivers

Available for: macOS Sonoma

Impact: An app may be able to disclose kernel memory

Description: The issue was addressed with improved bounds checks.

CVE-2025-24256: Murray Mike, Anonymous working with Trend Micro Zero Day Initiative

GPU Drivers

Available for: macOS Sonoma

Impact: An app may be able to cause unexpected system termination or corrupt kernel memory

Description: An out-of-bounds write issue was addressed with improved bounds checking.

CVE-2025-24273: Wang Yu of Cyberserval

CVE-2025-30464: ABC Research s.r.o.

ImageIO

Available for: macOS Sonoma

Impact: Parsing an image may lead to disclosure of user information

Description: A logic error was addressed with improved error handling.

CVE-2025-24210: Anonymous working with Trend Micro Zero Day Initiative

Installer

Available for: macOS Sonoma

Impact: An app may be able to check the existence of an arbitrary path on the file system

Description: A permissions issue was addressed with additional sandbox restrictions.

CVE-2025-24249: YingQi Shi(@Mas0nShi) of DBAppSecurity's WeBin lab and Minghao Lin (@Y1nKoc)

Installer

Available for: macOS Sonoma

Impact: A sandboxed app may be able to access sensitive user data

Description: A logic issue was addressed with improved checks.

CVE-2025-24229: an anonymous researcher

Kerberos Helper

Available for: macOS Sonoma

Impact: A remote attacker may be able to cause unexpected app termination or heap corruption

Description: A memory initialization issue was addressed with improved memory handling.

CVE-2025-24235: Dave G.

Kernel

Available for: macOS Sonoma

Impact: A malicious app may be able to attempt passcode entries on a locked device and thereby cause escalating time delays after 4 failures

Description: A logic issue was addressed with improved state management.

CVE-2025-30432: Michael (Biscuit) Thomas - @biscuit@social.lol

Kernel

Available for: macOS Sonoma

Impact: An app may be able to modify protected parts of the file system

Description: The issue was addressed with improved checks.

CVE-2025-24203: Ian Beer of Google Project Zero

Kernel

Available for: macOS Sonoma

Impact: An attacker with user privileges may be able to read kernel memory

Description: A type confusion issue was addressed with improved memory handling.

CVE-2025-24196: Joseph Ravichandran (@0xjprx) of MIT CSAIL

LaunchServices

Available for: macOS Sonoma

Impact: A malicious JAR file may bypass Gatekeeper checks

Description: This issue was addressed with improved handling of executable types.

CVE-2025-24148: Kenneth Chew

Libinfo

Available for: macOS Sonoma

Impact: A user may be able to elevate privileges

Description: An integer overflow was addressed with improved input validation.

CVE-2025-24195: Paweł Płatek (Trail of Bits)

libxml2

Available for: macOS Sonoma

Impact: Parsing a file may lead to an unexpected app termination

Description: This is a vulnerability in open source code and Apple Software is among the affected projects. The CVE-ID was assigned by a third party. Learn more about the issue and CVE-ID at cve.org.

CVE-2025-27113

CVE-2024-56171

libxpc

Available for: macOS Sonoma

Impact: An app may be able to break out of its sandbox

Description: This issue was addressed through improved state management.

CVE-2025-24178: an anonymous researcher

libxpc

Available for: macOS Sonoma

Impact: An app may be able to delete files for which it does not have permission

Description: This issue was addressed with improved handling of symlinks.

CVE-2025-31182: 风沐云烟(@binary_fmyy) and Minghao Lin(@Y1nKoc), Alex Radocea and Dave G. of Supernetworks

libxpc

Available for: macOS Sonoma

Impact: An app may be able to gain elevated privileges

Description: A logic issue was addressed with improved checks.

CVE-2025-24238: an anonymous researcher

Mail

Available for: macOS Sonoma

Impact: "Block All Remote Content" may not apply for all mail previews

Description: A permissions issue was addressed with additional sandbox restrictions.

CVE-2025-24172: an anonymous researcher

manpages

Available for: macOS Sonoma

Impact: An app may be able to access sensitive user data

Description: This issue was addressed with improved validation of symlinks.

CVE-2025-30450: Pwn2car

Maps

Available for: macOS Sonoma

Impact: An app may be able to read sensitive location information

Description: A path handling issue was addressed with improved logic.

CVE-2025-30470: LFY@secsys from Fudan University

NSDocument

Available for: macOS Sonoma

Impact: A malicious app may be able to access arbitrary files

Description: This issue was addressed through improved state management.

CVE-2025-24232: an anonymous researcher

OpenSSH

Available for: macOS Sonoma

Impact: An app may be able to access user-sensitive data

Description: An injection issue was addressed with improved validation.

CVE-2025-24246: Mickey Jin (@patch1t)

PackageKit

Available for: macOS Sonoma

Impact: An app may be able to modify protected parts of the file system

Description: The issue was addressed with improved checks.

CVE-2025-24261: Mickey Jin (@patch1t)

PackageKit

Available for: macOS Sonoma

Impact: An app may be able to modify protected parts of the file system

Description: A logic issue was addressed with improved checks.

CVE-2025-24164: Mickey Jin (@patch1t)

PackageKit

Available for: macOS Sonoma

Impact: A malicious app with root privileges may be able to modify the contents of system files

Description: A permissions issue was addressed with additional restrictions.

CVE-2025-30446: Pedro Tôrres (@t0rr3sp3dr0)

Parental Controls

Available for: macOS Sonoma

Impact: An app may be able to retrieve Safari bookmarks without an entitlement check

Description: This issue was addressed with additional entitlement checks.

CVE-2025-24259: Noah Gregory (wts.dev)

Photos Storage

Available for: macOS Sonoma

Impact: Deleting a conversation in Messages may expose user contact information in system logging

Description: A logging issue was addressed with improved data redaction.

CVE-2025-30424: an anonymous researcher

Power Services

Available for: macOS Sonoma

Impact: An app may be able to break out of its sandbox

Description: This issue was addressed with additional entitlement checks.

CVE-2025-24173: Mickey Jin (@patch1t)

Sandbox

Available for: macOS Sonoma

Impact: An input validation issue was addressed

Description: The issue was addressed with improved checks.

CVE-2025-30452: an anonymous researcher

Sandbox

Available for: macOS Sonoma

Impact: An app may be able to access protected user data

Description: A permissions issue was addressed with additional restrictions.

CVE-2025-24181: Arsenii Kostromin (0x3c3e)

Security

Available for: macOS Sonoma

Impact: A remote user may be able to cause a denial-of-service

Description: A validation issue was addressed with improved logic.

CVE-2025-30471: Bing Shi, Wenchao Li, Xiaolong Bai of Alibaba Group, Luyi Xing of Indiana University Bloomington

Security

Available for: macOS Sonoma

Impact: A malicious app acting as a HTTPS proxy could get access to sensitive user data

Description: This issue was addressed with improved access restrictions.

CVE-2025-24250: Wojciech Regula of SecuRing (wojciechregula.blog)

Share Sheet

Available for: macOS Sonoma

Impact: A malicious app may be able to dismiss the system notification on the Lock Screen that a recording was started

Description: This issue was addressed with improved access restrictions.

CVE-2025-30438: Halle Winkler, Politepix theoffcuts.org

Shortcuts

Available for: macOS Sonoma

Impact: An app may be able to access user-sensitive data

Description: An access issue was addressed with additional sandbox restrictions.

CVE-2025-24280: Kirin (@Pwnrin)

Shortcuts

Available for: macOS Sonoma

Impact: A Shortcut may run with admin privileges without authentication

Description: An authentication issue was addressed with improved state management.

CVE-2025-31194: Dolf Hoegaerts

Shortcuts

Available for: macOS Sonoma

Impact: A shortcut may be able to access files that are normally inaccessible to the Shortcuts app

Description: A permissions issue was addressed with improved validation.

CVE-2025-30465: an anonymous researcher

Shortcuts

Available for: macOS Sonoma

Impact: A shortcut may be able to access files that are normally inaccessible to the Shortcuts app

Description: This issue was addressed with improved access restrictions.

CVE-2025-30433: Andrew James Gonzalez

Siri

Available for: macOS Sonoma

Impact: An attacker with physical access may be able to use Siri to access sensitive user data

Description: This issue was addressed by restricting options offered on a locked device.

CVE-2025-24198: Richard Hyunho Im (@richeeta) with routezero.security

Siri

Available for: macOS Sonoma

Impact: An app may be able to access sensitive user data

Description: The issue was addressed with improved restriction of data container access.

CVE-2025-31183: Kirin (@Pwnrin), Bohdan Stasiuk (@bohdan_stasiuk)

Siri

Available for: macOS Sonoma

Impact: An app may be able to access user-sensitive data

Description: An authorization issue was addressed with improved state management.

CVE-2025-24205: YingQi Shi(@Mas0nShi) of DBAppSecurity's WeBin lab and Minghao Lin (@Y1nKoc)

SMB

Available for: macOS Sonoma

Impact: Mounting a maliciously crafted SMB network share may lead to system termination

Description: A race condition was addressed with improved locking.

CVE-2025-30444: Dave G.

SMB

Available for: macOS Sonoma

Impact: An app may be able to execute arbitrary code with kernel privileges

Description: A buffer overflow issue was addressed with improved memory handling.

CVE-2025-24228: Joseph Ravichandran (@0xjprx) of MIT CSAIL

smbx

Available for: macOS Sonoma

Impact: An attacker in a privileged position may be able to perform a denial-of-service

Description: The issue was addressed with improved memory handling.

CVE-2025-24260: zbleet of QI-ANXIN TianGong Team

Software Update

Available for: macOS Sonoma

Impact: A user may be able to elevate privileges

Description: This issue was addressed with improved validation of symlinks.

CVE-2025-24254: Arsenii Kostromin (0x3c3e)

Spotlight

Available for: macOS Sonoma

Impact: An app may be able to access sensitive user data

Description: A permissions issue was addressed with additional sandbox restrictions.

CVE-2024-54533: Csaba Fitzl (@theevilbit) of OffSec

Storage Management

Available for: macOS Sonoma

Impact: An app may be able to enable iCloud storage features without user consent

Description: A permissions issue was addressed with additional restrictions.

CVE-2025-24207: 风沐云烟 (binary_fmyy) and Minghao Lin (@Y1nKoc), YingQi Shi (@Mas0nShi) of DBAppSecurity's WeBin lab

StorageKit

Available for: macOS Sonoma

Impact: An app may be able to gain root privileges

Description: A permissions issue was addressed with additional restrictions.

CVE-2025-30449: an anonymous researcher, Arsenii Kostromin (0x3c3e)

StorageKit

Available for: macOS Sonoma

Impact: An app may be able to access protected user data

Description: This issue was addressed with improved handling of symlinks.

CVE-2025-24253: Mickey Jin (@patch1t), Csaba Fitzl (@theevilbit) of Kandji

StorageKit

Available for: macOS Sonoma

Impact: An app may be able to bypass Privacy preferences

Description: A race condition was addressed with additional validation.

CVE-2025-31188: Mickey Jin (@patch1t)

StorageKit

Available for: macOS Sonoma

Impact: An app may be able to access user-sensitive data

Description: A race condition was addressed with additional validation.

CVE-2025-24240: Mickey Jin (@patch1t)

System Settings

Available for: macOS Sonoma

Impact: An app may be able to access protected user data

Description: This issue was addressed with improved validation of symlinks.

CVE-2025-24278: Zhongquan Li (@Guluisacat)

SystemMigration

Available for: macOS Sonoma

Impact: A malicious app may be able to create symlinks to protected regions of the disk

Description: This issue was addressed with improved validation of symlinks.

CVE-2025-30457: Mickey Jin (@patch1t)

Voice Control

Available for: macOS Sonoma

Impact: An app may be able to access contacts

Description: This issue was addressed with improved file handling.

CVE-2025-24279: Mickey Jin (@patch1t)

WindowServer

Available for: macOS Sonoma

Impact: An attacker may be able to cause unexpected app termination

Description: A type confusion issue was addressed with improved checks.

CVE-2025-24247: PixiePoint Security

WindowServer

Available for: macOS Sonoma

Impact: An app may be able to trick a user into copying sensitive data to the pasteboard

Description: A configuration issue was addressed with additional restrictions.

CVE-2025-24241: Andreas Hegenberg (folivora.AI GmbH)

Xsan

Available for: macOS Sonoma

Impact: An app may be able to cause unexpected system termination

Description: A buffer overflow was addressed with improved bounds checking.

CVE-2025-24266: an anonymous researcher

Xsan

Available for: macOS Sonoma

Impact: An app may be able to cause unexpected system termination

Description: An out-of-bounds read was addressed with improved bounds checking.

CVE-2025-24265: an anonymous researcher

Xsan

Available for: macOS Sonoma

Impact: An app may be able to cause unexpected system termination or corrupt kernel memory

Description: A buffer overflow issue was addressed with improved memory handling.

CVE-2025-24157: an anonymous researcher

Additional recognition

AirPlay

We would like to acknowledge Uri Katz (Oligo Security) for their assistance.

Entry added April 28, 2025

Audio

We would like to acknowledge Hossein Lotfi (@hosselot) of Trend Micro Zero Day Initiative for their assistance.

Security

We would like to acknowledge Kevin Jones (GitHub) for their assistance.

Shortcuts

We would like to acknowledge Chi Yuan Chang of ZUSO ART and taikosoup for their assistance.

SMB

We would like to acknowledge Dave G. for their assistance.

Published Date: April 29, 2025